

## **Council of Defense and Space Industry Associations**

1000 Wilson Blvd., Suite 1800

Arlington, VA 22209

[www.codsia.org](http://www.codsia.org)

(703) 243-2020

October 12, 2005

Ms. Debra Overstreet  
Defense Acquisition Regulations Council  
OUSD(AT&L)DPAP(DAR)  
IMD 3C132  
3062 Defense Pentagon  
Washington, DC 20301-3062

Ref: DFARS Case 2004-D010 (Export-Controlled Information and Technology)  
CODSIA Case No 05-05

By email: [dfars@osd.mil](mailto:dfars@osd.mil)

Dear Ms. Overstreet:

On behalf of the Council of Defense and Space Industry Associations (CODSIA), we are pleased to submit comments on the referenced proposed rule, published in the *Federal Register* on July 12, 2005 (70 F.R. 39976, *et. seq.*). The proposed rule would amend the Defense Federal Acquisition Regulations Supplement (DFARS) to address requirements for preventing unauthorized disclosure of export-controlled information and technology under Department of Defense (DOD) contracts. Specifically, this DFARS change proposes to add a new DFARS Subpart 204.73, and an associated new contract clause, that would require contractors to: (1) comply with all applicable laws and regulations regarding export-controlled information and technology; (2) maintain an effective export compliance program; (3) conduct initial and periodic training on export compliance controls; and (4) perform periodic assessments.

Formed in 1964 by the industry associations with common interests in the defense and space fields, CODSIA is currently composed of six associations representing over 4,000 member firms across the nation. Participation in CODSIA projects is strictly voluntary. A decision by any member association to abstain from participating in a particular activity is not necessarily an indication of dissent.

### **Principal Comments**

We understand that the proposed rule and clause have been issued as the result of findings and recommendations contained in a March 25, 2004, DOD Inspector General (IG) Report which found that the DOD did not have adequate processes to identify unclassified export-controlled information and technology and to ensure that contractors, among others, are preventing unauthorized disclosure of such information to foreign nationals. While we recognize that contractor compliance with export control laws and regulations is an extremely important contractor responsibility, we believe that the proposed rule goes well beyond the need identified by the IG and further complicates an already complex area. This proposed additional regulation of export control is

unnecessary since DOD already possesses adequate contractual and legal enforcement tools to protect against the risks identified by the IG to sufficiently identify unclassified export-controlled information and technology and to prevent unauthorized disclosure of such. Moreover, it remains appropriate to leave compliance enforcement with the complex set of export control laws and regulations to the United States Departments of State and Commerce. These agencies have the statutory authority and subject matter expertise to efficiently and consistently enforce the complex laws and regulations that apply to export compliance. For these reasons, and based on the detailed comments below, we urge the DAR Council to withdraw this rule in its entirety. Our major arguments in justification for withdrawal appear below.

***Jurisdictional objections.***—DOD’s proposal is inconsistent with existing U.S. Department of State (State) and U.S. Department of Commerce (Commerce) export control laws and regulations. The vast majority of our member companies already maintain robust export compliance programs. We believe this additional layer of regulation and requirements related to export control by DOD is duplicative and unnecessary. Our overarching concern is that the proposed rule, if adopted, imposes audit and enforcement requirements by the DOD which are already addressed in U.S. export control regulations which are under the jurisdiction of the State and Commerce Departments. Additionally, we are concerned that some language in the new proposed rule is contrary to existing U.S. export control regulations. Furthermore, the proposed rule imposes requirements on the exporter that go beyond compliance requirements under the U.S. export control regulations administered by the State and Commerce Departments. All of this gives rise to inconsistencies and the potential for significant ambiguities across all three regulatory regimes (State, Commerce, and DOD) that may be fatal to any contractor’s export control compliance program. On these bases alone, we strongly urge that the rule be withdrawn in its entirety.

***DOD has adequate contractual and legal enforcement tools.***--Additional enforcement tools are unnecessary since DOD already possesses the enforcement tools of termination for default and/or suspension or debarment of a contractor who violates export laws or regulations. A defense contractor whose ability to export has been extinguished by State or Commerce Department enforcement action will quickly find itself unable to make adequate progress under its contract and therefore subject to the Termination for Default clause (FAR 52.249-8) of the contract. Likewise, a contractor which violates export control laws is subject to suspension and debarment under FAR 9.407-2 and FAR 9.406-2 for having committed an “offense indicating a lack of business integrity or business honesty that seriously and directly affects the public responsibility of a Government contractor or subcontractor.” Additional enforcement tools are unnecessary for DOD. Under the proposed DFARS rule, a contractor may become exposed to suspension and debarment for a much broader array of conduct unrelated to any actual violation of the export laws.

***Proposed DFARS rule is fatally flawed.***--The proposed rule is excessive and impracticable. It not only tells contractors what to do, it prescribes how to do it which, essentially, imposes a government design on a contractor’s compliance program. The problem is that contractor export control compliance programs are not conducive to a “one size fits all” portfolio but rather must be tailored to individual company needs. Additionally, under the proposed regulations, the contracting officer is obligated to ensure that contracts identify any export controlled information and technology, as determined by the requiring activity. Without extensive training and experience, it would be difficult for the contracting officer to know what information and technology are subject to export controls, under either State or Commerce export control regulations or, just as importantly, to make export control jurisdiction determinations. The complex

nature of these determinations could result in one contracting officer making a determination that would be inconsistent with another contracting officer's determination, or the determination of State, which could create an uneven playing field for defense contractors. Furthermore, it is possible that a DOD official could make export control determinations solely on the basis of national security considerations, rather than on an objective legal analysis of the applicable regulations. While national security considerations are a critical part of export approval decisions, they should not apply when making regulatory compliance determinations. Again, we ask that the rule be withdrawn in its entirety.

### **Specific, Detailed Comments**

In addition to considering our principal comments presented above, we ask that you consider specific, detailed comments that we have provided as an attachment to this letter and expressly incorporate into this letter in further support of our opposition to the proposed rule and clause. These detailed comments point up additional significant deficiencies in the rule that underscore why the rule must be withdrawn or completely revised. (Attachment A).

### **Alternative to this rule**

Without conceding our position that the rule should be withdrawn, should the DAR Council determine that some amending language must be incorporated into the DFARS to address the IG's recommendations, we suggest that a relatively brief rule and clause could be adopted which alerts contracting officers and contractors to the export control requirements of the State Department's International Traffic in Arms Regulations (ITAR, 22 C.F.R. parts 120-130) and the Commerce Department's Export Administration Regulations (EAR, 15 C.F.R. parts 730-774). This would avoid the duplication of language and conflicts referred to above. There are precedents for this approach such as when the FAR implemented the security requirements of the National Industrial Security Program Operating Manual (NISPOM) by simply alerting contractors that the NISPOM was a requirement (see FAR part 52.204-2). A similar approach was adopted through the FAR implementation of the Privacy Act (see FAR 52.224-1). We welcome an opportunity to share suggested textual language if DOD elects this course of action. In any event, should DOD decide that it will adopt a DFARS Export rule that is significantly different from the proposed rule, we would expect that revised rule would be republished for additional public comment.

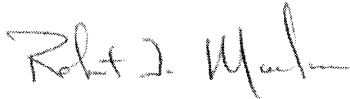
### **Conclusion**

In summary, we maintain that the Departments of State and Commerce, which have jurisdiction over and administer the transfer and control of exports of technology to foreign persons, should be the exclusive agencies to direct requirements, conduct audits, and enforce compliance with U.S. export control laws and regulations—not DOD. We also believe that DOD already possesses the necessary contractual and legal enforcement tools to identify export-controlled information and technology, to protect against improper disclosure of such information, and to impose appropriate sanctions against contractors for violations of export control laws and regulations. Finally, the DFARS proposal, as drafted, is fatally flawed and would greatly increase the risk of contract violations and sanctions to contractors where no export violation has occurred. For all of the reasons set forth in this letter and its attachment, as incorporated, we urge the DAR Council to withdraw the proposed rule in its entirety. In the alternative, the proposed rule should be significantly redrafted to simply reflect a recognition that contracting officers and contractors must be aware of and adhere to U.S. export control regulations pertaining

to export-controlled information and technology relative to DOD contracts, as contained in the State Department's ITAR and the Commerce Department's EAR.

Thank you for your attention to these comments. If you have any questions or need any additional information, please contact Elaine Guth of the Aerospace Industries Association (AIA), who serves as our point of contact for this matter. Elaine can be reached at (703) 358-1045 or at [elaine.guth@aia-aerospace.org](mailto:elaine.guth@aia-aerospace.org).

Sincerely,



Robert T. Marlow  
Vice President – Procurement and Finance  
Aerospace Industries Association



Dan Heinemeier  
President  
GEIA  
Electronic Industries Alliance



Peter Steffes  
Vice President – Government Policy  
National Defense Industrial Association



Alan Chvotkin  
Senior Vice President & Counsel  
Professional Services Council



Chris Jahn  
President  
Contract Services Association

Attachment

**Ref: DFARS Case 2004-D010 (Export-Controlled Information and Technology)  
CODSIA Case No. 05-XX**

As noted in our main letter, CODSIA believes the proposed rule is unnecessary and likely to cause more, not less confusion with regard to this very complex subject. Below are specific comments that identify the key elements of the proposed rule that are inconsistent with existing Department of State or Department of Commerce policy or will lead to greater confusion. We strongly recommend a much simpler notification of export requirements rather than establishing yet another set of duplicative and often inconsistent requirements.

***Specific, Detailed CODSIA Comments in Opposition to the Proposed DFARS Rule and Clause:***

**Comments on Part 204. – Administrative Matters**

**204.73—Export-Controlled Information and Technology at Contractor, University, and Federally Funded Research and Development Center Facilities**

1. **“Home country” reference is vague and inaccurate:** Proposed DFARS section 204.7302 of the proposed rule includes the following restrictive statement: “Any access to export-controlled information or technology by a foreign national or a foreign person anywhere in the world, including the United States, is considered an export to the home country of the foreign national or foreign person.” This apparent reference to the “deemed export rule” is confusing and misleading, without specific reference to the applicable provisions of the EAR and ITAR. “Home country” could be construed as the country of birth, rather than the country of which a foreign person is a national; if it is so construed, this is not an accurate statement of the law as it currently exists. Additionally, this general statement fails to take into account the differences between the ITAR and EAR with respect to the treatment of foreign nationals (including, for instance, with respect to dual nationals).
2. **Improper application of the terms “foreign person” and “foreign national”:** The terms foreign person and foreign national are not interchangeable within the context of U.S. export control regulations as they apply to persons who have permanent residence in the U.S. as defined by 8 U.S.C. 1101(a)(20) or who are protected individuals in the U.S. as defined by 8 U.S.C. 1324(b)(a)(3). Under the ITAR and the EAR, the definition of foreign person does not include a lawfully admitted permanent resident or an otherwise protected individual (such as a foreign national granted asylum in the U.S.). Permanent residents or otherwise protected individuals are considered U.S. persons for purposes of export controls, and access to export controlled information or technology by a permanent resident or otherwise protected individual is not an export. The term “foreign national,” on the other hand, may capture a permanent resident or otherwise protected individuals. By referring to “foreign persons” and “foreign nationals,” without distinction between the two, the proposed rule could in fact change the definition of export by designating as an export the transfer of export controlled information or technology to permanent residents or otherwise protected individuals and therefore requiring that they be treated as foreign persons for purposes of the

export control regulations whenever a DOD contract is involved. This will have significant legal implications for contractors in applying ITAR export requirements to non-ITAR foreign persons. A suggested clarification would be to delete all references to the term “foreign national” and add the ITAR definition of “foreign person” to the proposed clause.

3. **Inappropriate incorporation of DOD PGI into DFARS guidance:** The last sentence of proposed DFARS section 204.7302 of the proposed rule refers to “additional information relating to restrictions on export-controlled information and technology” to be found at “PGI 204.7302.” DOD PGI (Procedures, Guidance and Information) is intended for internal DOD use while DFARS is to contain only requirements of law, DOD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect beyond the internal operating procedures of DOD or “a significant cost or administrative impact on contractors or offerors.” (underline added)(DFARS 201.301(a)(v)). To the extent that the proposed PGI guidance is to contain additional restrictions on export-controlled information and technology, this is not an appropriate use of PGI because it may address material designed for DFARS inclusion—i.e., having a significant administrative impact on contractors and offerors. We recommend that any use of PGI for guidance on export-control restrictions be carefully reviewed for compliance with DFARS 201.301. Further, if PGI is referenced as a source for export-control restrictions, a reference to ITAR and EAR also should be added.

As noted in paragraphs 1-3, above, there are significant issues with the proposed language in 204.7302 which tries to summarize complex regulations without ever mentioning that there are already extensive requirements in existence under the authority of State and Commerce. The “General” paragraph should be replaced with the following:

“U.S. export control laws and regulations prohibit the unauthorized export of designated types of information and technology. The applicable restrictions are set forth in the International Traffic in Arms Regulations (22 CFR parts 120-130) (“ITAR”) and the Export Administration Regulations (15 CFR parts 730-774) (“EAR”).”

4. **Vague and unworkable policy statement:** Proposed DFARS section 204.7303 vests the contracting officer with oversight responsibility to “ensure that contracts identify any export-controlled information and technology, as determined by the requiring activity.” This may be an unworkable requirement, especially on a research and development contract at the time of award. All of the technologies to be used may not be known at that time. Any serious attempt to meet this standard could easily result in a very large list, requiring a great effort to compile and keep current. Catchall listings such as “Technologies and equipment on the USML or CCL” would be meaningless.

Additionally, we note that the “requiring activity” is not defined, but it should be, or at least clarified. In any event, requiring activities do not determine the entire content of contracts; their contributions may be limited to only portions of a contract. Moreover, the requirement to identify export-controlled information and technology may be difficult for even the requiring activity. It will require ITAR/EAR-trained personnel and additional review time. This determination requirement also raises issues as to responsibility for inadvertent export of export-

controlled information or technology that was not identified in the contract by the requiring activity. Finally, it is not clear how a requiring activity will determine which contracts are likely to involve “export-controlled information and technology” or whether affected contractors would have a right to petition such a determination, including through recourse to the EAR product classification or ITAR commodity jurisdiction processes. We recommend that this section be deleted or the following language substituted in its place:

“The contracting officer shall provide notice to contractors when a contract is known or expected to contain export-controlled information or technology or the contractor, in contract performance, is expected to use or generate export-controlled information or technology. Such notice is met by the inclusion of the clause at 252.204-70XX.”

5. **Application of clause is overreaching:** The proposed rule, in section 204.7304, states that the new clause is to be used in solicitations and contracts for: (a) research and development (R&D); or (b) services or supplies that may involve the use or generation of export-controlled information or technology. This is excessive and overreaching since many R&D contracts may not involve export-controlled technology at all and because it imposes controls on services/supply contracts that merely “may” involve export-controlled technology. As we note elsewhere, the new rule fails to establish a mechanism for establishing which contracts actually involve ITAR or EAR-controlled technology or a mechanism by which contractors may contest such a determination. Alternatively, it may make more sense to add a “check-the-box” in Section K of the solicitation as to whether the offeror/bidder intends to use or generate export-controlled information in the performance of the contract.

## Comments on Part 252 – Solicitation Provisions and Contract Clauses

### 252.204-70XX Requirements Regarding Access to Export-Controlled Information and Technology

6. **Definition of “export controlled information and technology” is unclear:** The proposed definition in Subpart 252.204-70XX(a) of “export controlled information and technology” is unclear and lacks any connection to the operative definitions of technical data contained in the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR). The terms “information” and “technology” are not defined anywhere in Part 120 of the ITAR, although ITAR Section 120.10 defines “technical data” subject to export control. Likewise, the term “information” is not defined in Part 772 of the EAR, and the term “technology” is defined only in the context of “technical data” or “technical assistance” in EAR Part 772. The proposed DFARS subpart 252.204 definition of what is covered should be revised to be consistent with the operative ITAR and EAR definitions of technical data.
7. **Conflicts in determining an effective compliance program:** The proposed regulation in section 252.204-70XX(d) directs contractors to maintain “effective export compliance programs,” and specifically requires “adequate controls” over physical, visual and electronic access to export-controlled technical data. However, it is unclear from the rule whether or how DCMA or any other administering body would assess the effectiveness or adequacy of contractors’

internal control programs. In order to remain compliant with U.S. State and Commerce export control regulations and avoid violations which could result in severe enforcement actions, companies subject to such regulations have in place a compliance program which under the authority of the ITAR or the EAR permit the agencies to conduct audits at their discretion. Additionally, the establishment of Technology Control Plans (TCPs) (Department of State), Technology Transfer Control Plans (TTCPs) (Department of Defense) and Internal Control Plans (ICPs) (Department of Commerce) is often a requirement of export approvals. These plans have strict requirements for the control of foreign persons, exchange of technical data and general compliance and record keeping requirements. In the case of exports of technology to foreign persons who are employed by a U.S. company, control plans are always a condition of the license. As part of its audits, the agency of jurisdiction looks into the company's processes related to export controls, e.g., compliance with the provisions of a license, license maintenance, recordkeeping, foreign person access, employee training, etc. For DOD to impose similar requirements under the DFARS is duplicative at a minimum. A more serious consequence would be a disruption of operations due to additional audits and consequently the possibility of punitive actions affecting the contract.

8. **Separate badging requirements for foreign nationals and foreign persons is overreaching:** The lack of distinction in the rule between "foreign nationals" and "foreign persons" (noted earlier) is compounded further by the rule's requirement in Section 252.204-70XX(d)(1) for "unique badging requirements" which would entail separate badging for foreign nationals and foreign persons. Not all companies use a separate badging system to identify foreign persons (as well as a system that treats foreign persons differently from foreign nationals). The proposed rule would mandate contractors to incur a cost of setting up a new badging system regardless of the adequacy of any existing system they may have. This new badging requirement is not an ITAR or EAR requirement. In many instances, the costs of these new badging requirements could be significant. The impact could be substantial to a small business trying to enter the defense market.
9. **Segregated work areas for foreign persons should be contractor-determined:** The requirement at section 252.204-70XX(d)(1) to have segregated work areas for export-controlled information and technology may be plausible in some cases; for example, an assembly line disclosing export controlled information or technology must be protected from unauthorized access by foreign persons. On the other hand, to have foreign persons physically separated might not be necessary if access can be controlled by other means (for example, where access to controlled technology is through electronic access that is properly restricted through a contractor's IT security system). The company implementing its export compliance program, not the contracting officer or any other DOD administrative officer, is best qualified to determine in which manner the disclosure of controlled information or technology must be protected, and the most secure and cost efficient method to be used.
10. **Access contingent upon authorization or exemption is overreaching:** The proposed clause, at subsection (d)(2), dictates that a "contractor shall not allow access by foreign nationals or foreign persons to export-controlled information and technology without obtaining an export license, other authorization, or exemption." This provision is too broad. It starts from the assumption that any of the technology at issue could only be released to the company's foreign national employees with the benefit of some form of "authorization" or "exemption." This provision improperly presumes that access control measures are necessary



without establishing the nature of the technology at issue and the status/mix of a contractor's workforce.

11. **Training and periodic assessments are contractor best practices and should not be requirements:** The proposed DFARS clause dictates additional training requirements in 252.204-70XX(e)(1) and periodic assessment requirements in subsection (e)(2)—these will likely add to contractors' costs and, accordingly, DOD's costs. Contractors routinely conduct such training and assessments as part of their compliance with ITAR and EAR provisions, but they are not affirmatively required by the EAR or ITAR. The clause exceeds existing law and attempts to codify through contract a best practice in industry. Moreover, the nature, scope and frequency of such training and assessment should also be tied to the particular circumstances of the company and technologies at issue. A contractual stipulation to this effect is unnecessary. Additionally, in the case of periodic assessments, it would appear that contractors will become responsible for reviewing and monitoring their suppliers' and subcontractors' export compliance in those instances where the proposed clauses must be flowed down under 252.204-70XX(g)(2). Again, this is an additional, unnecessary requirement that is likely to increase government and contractor costs.

## General Comments

12. **Increased contractor risk with audits and enforcement:** As the arm of the DOD that oversees contract compliance, the Defense Contract Management Agency (DCMA) has authority to conduct audits and to take action pursuant to findings. It is expected that if the proposed regulations are changed to include ITAR and EAR provisions, audit and enforcement will fall within their purview. The DCMA does not have the expertise to assess compliance with the ITAR and the EAR, a capability that cannot be acquired with only basic training. Further, the DCMA does not have the principal statutory authority to take action for non-compliance with the ITAR or the EAR. Adding to the complexity of the implementation is the fact that most major defense contractors have multiple facilities and support more than one military customer or program in each facility. Requiring each PCO and each cognizant DCMA to drive export compliance will most certainly lead to overlapping audits, inconsistent findings and additional cost without significant impact on overall compliance. As a result, companies could find themselves having to spend additional time and money responding to audits by a variety of agencies (State, Commerce, DCMA) and explaining its actions to contracting officers who may have only a rudimentary understanding of the complex export requirements. Worse, companies could be subject to contract suspension or other breach of contract actions pursuant to decisions made by officials who may have neither the expertise to assess nor the authority to act upon actions related to compliance with the U.S. export control regulations.
13. **Contractor liability concerns:** The proposed language is silent on contractor liability, making it unclear as to what approach contractors must take in the event of an unauthorized export when the submittal of a voluntary disclosure to the State Department's Directorate of Defense Trade Controls or Commerce Department's Office of Export Enforcement would be appropriate. There are well-defined steps today under both the ITAR and EAR for the submittal of voluntary disclosures. It is not clear whether the proposed clause will require a contractor to make disclosures through the DOD contracting officer or whether the existing routes through the State and Commerce Departments will continue to

be appropriate. It also is not clear whether the contractor will be liable under the regulations of the Defense Criminal Investigative Service.

14. **Increased costs to defense products:** Adoption of the proposed regulation would increase costs in defense procurement. The Defense Contract Audit Agency's (DCAA) audit manual would most certainly be expanded to contain an audit routine dedicated to export control. A contractor would have to adopt expensive and wasteful processes in order to prove its compliance with the proposed broad requirements. It is important to distinguish between contractor expenditure of funds necessary to comply with State and Commerce Department export control requirements to ensure adequate compliance against the proposed DOD regime. Under this new regime, contractors would have to spend huge additional sums in order to prove compliance to the DCAA with proposed DFARS housekeeping procedures. These large additional expenditures would provide no additional value but merely increase the cost of defense products and services to the American taxpayer.
15. **Adverse impact to smaller businesses:** For smaller businesses which may be prime contractors or subcontractors, establishing an export compliance program in accordance with this proposed rule, to include training and periodic assessments, may be difficult and certainly costly. The imposition of separate badging requirements (discussed elsewhere) will also most likely create a difficult and adverse cost impact upon smaller businesses. DOD may wish to consider what role it will play in assisting small business in implementing this requirement.